UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,600	07/26/2001	Chris A. Barton	NAI1P020/01.139.01	8707

28875 7590 01/13/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,600	BARTON ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09042001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-39 have been considered.

Claim Objections

Claims 35 and 39 are objected to because of the following informalities: "units is" in part f) is a grammatical error. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Makita, U.S. Patent Application Publication No. 2001/0007120.

As per claims 1 and 17, the applicant describes a method for scanning read data from storage comprising the following limitations which are met by Makita:

a) receiving a request for data saved in storage from a central processing unit [0180];

b) scanning the requested data [0182];

c) transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning [0184];

The applicant describes an anti-virus scanning system in a storage subsystem which seeks to solve two problems as listed in the Background of the Invention. The first is to "combat viruses and other hostile content in memory subsystems" (Page 2), and the second is to alleviate

load from the processor by scanning in the subsystem because scanning by the processor "uses up a large proportion of system resources in the form of cycles in the central processing unit" (Page 2). Makita discloses an invention which meets all the limitations of the claims and meets both problems: "by providing the external storage with a virus check means to perform a virus check on a file to be recorded on a recording medium, it becomes unnecessary for the host computer to perform a virus check, thus reducing a processing load imposed on the host computer" [0062].

Regarding the use of a central processing unit, the primary reference discloses an operating system control unit. The operating system control unit embodies the CPU because it is well known in the art that an operating system runs on the central processing unit. The role of the operating system control unit of the primary reference is identical to the role of the CPU as described in the applicant's invention. The operating system control unit controls the read and write requests which take place between the host computer and the remote storage ([0008] and Fig 4). According to the applicant, the central processing unit issues read and write requests between the computer and the storage (Page 5).

As per claims 2 and 18, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage is selected from the group consisting of a hard drive, a compact disc-read only memory (CD-ROM), and a floppy disc ([0004], [0015], and Fig 4);

As can be seen in the paragraphs and figure referenced above, the storage of the primary reference is a hard drive.

As per claims 3,19, and 37, the applicant describes the method of claims 1,17, and 35 respectively, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning is performed by a scanning module coupled to a storage subsystem controller ([0091] and Fig 15);

The applicant should note that the scanning module is the virus check unit (413 of Fig 15) and the storage subsystem controller is the file management unit (Fig 211 of Fig 15). According to the applicant the "storage subsystem controller [is used] for controlling access, i.e. read, writes, etc., to the storage" (Page 5). According to the primary reference the "file management unit manages the storage of files into, the readout and deletion of files from, and access rights to the recording medium of the external storage" [0091].

As per claims 4 and 20, the applicant describes the method of claims 3 and 19, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit (Fig 15, [0010], Fig 4, [0010]);

The applicant should note the storage driver is the interface unit (21 of Fig 15). According to the applicant "the storage driver interfaces with the operating system running on the central processing unit for communicating the read and write requests to the storage subsystem controller" (Page 8). According to the primary reference the "interface unit exchanges data with the host computer" [0010].

As per claims 5 and 21, the applicant describes the method of claims 3 and 19, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage subsystem controller is coupled to the storage (Fig 15);

The applicant should note as described above, the storage subsystem controller is the file management unit (211 of Fig 15).

As per claims 6-7 and 22-23, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning module includes software ([0213] and Fig 15);

The primary reference discloses a scanning module unit which incorporates both software and hardware components. Regarding the software component, the primary reference discloses that the virus check can take the form of a program [0213]. Regarding the hardware component, the primary reference discloses the use of a segregated virus check unit which is connected to a plurality of other units, such as a storage unit (22 of Fig 15) and an interface unit (21 of Fig 15) in a bus-style system.

As per claims 8 and 24, the applicant describes the method of claims 3 and 19, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Further comprising allowing a user to disable the scanning module [0057];

The applicant should note that the primary reference includes the use of content scanning, which is used to determine a format of data and format the data to a user-selected format, and virus scanning, which is used to detect malicious data. The primary reference discloses the use of disabling the content scanning, or "formatting function", in the paragraph referenced above.

As per claims 9 and 25, the applicant limits the method of claims 8 and 24, which are anticipated by Makita (see above), with the following limitation which is also met by Makita:

Wherein data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module ([0057] and [0058]);

The applicant should note if the user does not set the operation of the formatting function, formatted data, or content data, is precluded from being transmitted from the storage to the cpu.

As per claims 10 and 26, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Further comprising executing an event based on results of the scanning [0183];

Two events are mentioned: halting the scanning/transmission of data process and alerting the user.

As per claims 11 and 27, the applicant describes the method of claims 10 and 26, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the event includes an alert [0183].

As per claims 12 and 28, the applicant describes the method of claims 10 and 26, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Further comprising disabling the scanning module in response to the event [0183];

The applicant should note that the scanning/transmission of data process is halted.

As per claims 13 and 29, the applicant describes the method of claims 12 and 28, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein data is precluded from being transmitted from the storage to the central processing unit upon disabling of the scanning module [0183];

As per claims 14 and 30, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning includes content scanning ([0054] and [0055]);

The applicant should note that the primary reference includes the use of content scanning, which is used to determine a format of data and format the data to a user-selected format, and virus scanning, which is used to detect malicious data.

As per claims 15 and 31, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning includes virus scanning [0182];

As per claims 16 and 32, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage is accessible via a network ([0036] and [0196] and Fig 19);

As described by the applicant, the system takes place in "an environment in which the storage device is connected to and/or disconnected from each of a plurality of host computers" [0036].

As per claims 33-34, the applicant discloses a method for scanning data written to storage comprising the following limitations:

a) receiving a request for data to be written in storage, the request being from a central processing unit [0174];

b) scanning the data [0174];

c) writing the data to the storage if malicious code is not found in the data during the scanning [0177];

As described earlier by the examiner, regarding the use of a central processing unit, the primary reference discloses an operating system control unit. The operating system control unit embodies the CPU as it is well known in the art that an operating system runs on the central processing unit. The role of the operating system control unit of the primary reference is identical

to the role of the CPU as described in the applicant's invention. The operating system control unit controls the read and write requests which take place between the host computer and the remote storage ([0008] and Fig 4). According to the applicant, the central processing unit issues read and write requests between the computer and the storage (Page 5).

As per claims 35 and 39, the applicant describes a system for scanning data read from storage comprising the following limitations which are met by the applicant:

a) storage for saving data therein (22 of Fig 15);

b) a storage subsystem controller coupled to the storage for controlling access to the data saved therein (211 of Fig 15);

c) a central processing unit coupled to the storage subsystem controller for issuing read requests for reading the data saved therein for processing purposes, and write requests for writing data to the storage (110 of Fig 15; 14 of Fig 4; [0008]);

d) a scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data in response to the requests (413 of Fig 15);

e) an event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning (211 of Fig 15; [0183]; [0091]);

f) wherein the central processing units is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning ([0183] and [0184]);

As described earlier by the examiner, regarding the use of a central processing unit, the primary reference discloses an operating system control unit. The operating system control unit embodies the CPU as it is well known in the art that an operating system runs on the central processing unit. The role of the operating system control unit of the primary reference is identical to the role of the CPU as described in the applicant's invention. The operating system control unit

controls the read and write requests which take place between the host computer and the remote storage ([0008] and Fig 4). According to the applicant, the central processing unit issues read and write requests between the computer and the storage (Page 5).

Regarding part e), the file management unit acts as the event manager module in addition to acting as the storage subsystem controller. The file management unit controls the transmission between the storage and the host computer [0091]. When a virus is detected, transmission between the remote storage and the host computer is halted [0183]. Since the file management unit executes the security event of halting the transmission between the storage and the host computer, the file management unit acts as the event manager module.

As per claim 36, the applicant limits the system of claim 35, which is anticipated by Makita (see above), with the following limitation which is also met by Makita:

Wherein the scanning module is coupled to the storage subsystem controller via a bus (Fig 15);

The primary reference discloses a connection between the scanning module, or virus check unit (413 of Fig 15), and the storage subsystem controller, or file management unit (211 of Fig 15) in a bus configuration where data is transferred between the segregated units.

As per claim 38, the applicant limits the system of claim 35, which is met by Makita (see above), with the following additional limitation which is also met by Makita:

Wherein the scanning module is coupled to the storage subsystem controller via a storage driver (Fig 15).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER